

Several news outlets reported on the Committee's [hearing to examine the government-wide transition to cloud computing](#). Chairman Towns held the hearing entitled, "Cloud Computing: Benefits and Risks of Moving Federal IT into the Cloud" on Thursday, July 1, 2010.

[Federal News Radio wrote](#) :

Federal agencies are under the gun to develop strategies for moving many of their IT functions into the cloud.

Rep. Edolphus Towns (D.-N.Y.), chairman of the House Oversight and Government Reform Committee, recognizes that moving the federal government to cloud computing may take as long as a decade and says his job is to see to it that risks and benefits are thoroughly weighed and balanced.

"It's clear to me that security and privacy are real concerns," Towns said in his opening statement. "Our natural impulse is to hold the things we value close to us, but cloud computing requires entrusting data to others." Towns acknowledges that in the long run, the government could also save money by using cloud computing...

White House Federal CIO Vivek Kundra came to offer an update on the effort to move federal agencies into the cloud, offering a somewhat dramatic graphic to underscore the urgency and the need for the change:

Unfortunately, the number of data centers in the United States Government has gone from 482 to over 1,100 in over a decade. While in the private sector, IBM went from 282 data centers to 12. That's not sustainable in the long term.

The Hill's Hillicon Valley blog [also reported on the hearing](#) :

Federal Chief Information Officer Vivek Kundra said the government spends a quarter of its \$80 billion annual IT budget on basic infrastructure such as hardware, software, electricity and personnel. He said shifting to the cloud could significantly lower those costs.

But Greg Wilshusen, director of information security issues at the Government Accountability Office, said agencies are concerned about relying on a private firm to house all their data. He said shifting applications to the cloud could create information security risks and leave agencies dependent on their cloud provider's security practices.

Wilshusen raised the possibility a cloud provider could fail to adequately delete data once their services are complete. The government could also lose control of its data if the company goes out of business or suffers a major security breach. He said agencies have expressed concerns about those scenarios and that risk could vary depending on the type of cloud network being deployed.